



H.R. 1817: The Homeland Security Authorization Act for Fiscal Year 2006

Committee on Homeland Security, Office of Communications
(202) 226-9600 <http://homeland.house.gov>

Defeating Terrorism

The primary missions of the Department of Homeland Security (DHS), established by the Homeland Security Act of 2002, are to:

- Prevent terrorist attacks
- Reduce vulnerability to terrorism
- Minimize damage and assist in recovery from terrorist attack

The Homeland Security Authorization Act for Fiscal Year 2006—the nation's first ever comprehensive annual Homeland Security authorization legislation—will help ensure that DHS has the resources and authority to achieve its missions.

Maximizing Homeland and Economic Security

Authorized Appropriations

The Department of Homeland Security is second only to the Department of Defense in discretionary spending of taxpayer money. The Administration requested \$34.2 billion for DHS for Fiscal Year 2006. The Department of Homeland Security Authorization Act enacts this request into law.

Planning for Prevention

- DHS has no department-wide plan solely focused on preventing a terrorist attack, while plans exist for attack response and securing infrastructure.
- The Act requires the Secretary of Homeland Security to develop and submit to Congress a Department of Homeland Security Terrorism Prevention Plan to set goals, objectives, and milestones to prevent acts of terrorism against the United States.

Mission-Based Budgeting

- The Fiscal Year 2006 DHS budget fails to provide sufficient data about the allocation of taxpayer dollars toward the missions Congress established for the Department.
- Future DHS budget requests must identify spending based on the DHS missions.

Preventing Attack

Deploying Counterterrorism Technology

- The Department of Homeland Security has yet to establish the centralized Technology Clearinghouse for advanced homeland security equipment and software Congress set forth in the Homeland Security Act of 2002.
- Terrorists will not wait for new technologies, but are working quickly to adapt existing technologies to their purposes.
- The Act requires the DHS Directorate of Science and Technology to create and establish a Technology Clearinghouse within 90 days to expedite the deployment of anti-terror technology for use by federal, state, local, and private sector officials.

Border Enforcement I: Security at the Line

- An insufficient number of Border Patrol agents leaves our land borders vulnerable to illegal crossings by terrorists.
- America's borders are the gateway for millions of visitors and for billions of dollars in trade; Congress must increase security without hindering legal international commerce and travel.
- The Act fully funds the recruitment and training of 2000 new border agents previously authorized in the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458).

Border Enforcement II: Focus on the Mission

- Two separate DHS agencies are responsible for enforcing border security: Customs and Border Patrol (CBP) and Immigration and Customs Enforcement (ICE). This creates unnecessary overlap and duplication of efforts, and significantly limits accountability.
- The Act requires the Secretary to review and report to Congress on the current structure and effectiveness of CBP and ICE operations; to develop a plan to correct the challenges created by the current division of CBP and ICE; and to consider options for combining redundant operations and personnel.

Streamlined Security Systems

- Multiple programs exist within DHS to expedite travel (Free and Secure Trade, Registered Traveler, and NEXUS/SENTRI) and provide background checks and security screenings for workers (Transportation Worker Identification Card and the Hazmat Endorsement Credential for drivers' licenses).
- These programs have separate application processes, fees, and enrollment facilities, yet they use many common resources and information for credentialing.
- The Act requires the Secretary to establish a single application program for conducting background checks on individuals participating in the programs.

Risk-Based Cargo Screening

- The Container Security Initiative (CSI), a DHS program placing Customs and Border Protection inspectors at selected foreign ports to target and inspect containers destined to the United States, currently covers 36 ports. Plans call for its expansion to approximately 50 ports in fiscal year 2005.
- CSI lacks a risk-based strategy. Initial port selection was based on shipping volume; future expansion should be risk-based.
- The Act requires the Secretary to conduct risk assessments at all foreign ports to determine the best allocation of resources in the future.

Red Teaming

- The Act broadens the intelligence process by requiring the use of red teams to help inform counterterrorism measures, particularly against nuclear and biological threats.

Priority on Personnel: IAIP Recruiting

- Successful and in-depth intelligence analysis requires highly trained and experienced professionals.
- The Act gives the Secretary the authority to provide incentives to recruit highly sought after intelligence analysts.

Nuclear and Biological Intelligence

- The key to preventing a nuclear or biological attack is intelligence. DHS lacks the robust intelligence capabilities required to detect nuclear threats in the planning and preparation stage and to develop means to pre-empt such efforts.
- The Act requires the establishment of analytic expertise within DHS to create and disseminate intelligence products specifically geared toward eliminating nuclear and biological threats.

Open Source Strategy

- DHS has no comprehensive open source intelligence strategy, despite broad agreement in the intelligence community that better open source intelligence will improve prevention capabilities.
- The Act establishes a “one stop shop” within DHS for reliable, comprehensive, and accessible open source information and analysis.

Information for Local Leaders

- Although the Secretary is required to disseminate threat warnings, other Federal agencies have issued security alerts without coordinating with DHS.
- This results in mixed messages being received by state and local officials, the media, and the public—and raises questions about federal credibility.
- The Act coordinates federal threat advisories by requiring that any threats be communicated in a manner that limits confusion and operational conflicts.

- It also formally authorizes the Homeland Security Information Network, a national, real time communication system for DHS and thousands of local agencies.

Being Prepared

Clarifying Threats and Colors

- The existing color-coded Threat Advisory System is vague, and warnings are overly broad, causing law enforcement and the public to discount the importance of the system.
- The Act reforms the Advisory System to communicate specific threat information directly to regions, states, localities, and private sector industries.
- This gives local and regional agencies the specific information they need to more effectively prevent, prepare for, and respond to acts of terror.

Exercise Goals

- Frequent and effective exercises are essential to terrorism preparedness at all levels of government.
- The Act creates a National Terrorism Exercise Program to coordinate and establish minimum standards for all federal, state, and local terrorism drills.
- The Act authorizes the biannual TOPOFF exercises to strengthen the nation's capacity to prevent, protect against, respond to, and recover from terrorist attacks—particularly catastrophic attacks.

Counter-Cyberterrorism

- The information infrastructure that controls much of the nation's vast physical resources and communications network remains highly vulnerable to terrorist attack.
- The Act elevates the cybersecurity mission in DHS by creating an Assistant Secretary for Cybersecurity in charge of the National Cybersecurity Office.
- The Assistant Secretary is tasked with developing a national cybersecurity response system, which will help detect, analyze, warn of, and respond to a cyber attack.
- The Act gives the Assistant Secretary authority over the National Communications System, recognizing the convergence of data and telephony.

Homeland Operations Collaboration

- Under the newly created 9/11 Memorial Homeland Security Fellows Program, state and local homeland security professionals will get first hand experience by working at the Homeland Security Operations Center.